Wreath products of cyclic p-groups as automorphism groups

Giovanni Cutolo
Università degli Studi di Napoli "Federico II", Dipartimento di Matematica e Applicazioni "R. Caccioppoli", Via Cintia — Monte S. Angelo, I-80126 Napoli, Italy.
e-mail: *cutolo@unina.it*

Howard Smith
Department of Mathematics, Bucknell University, Lewisburg, Pennsylvania 17837, USA.
e-mail: *howsmith@bucknell.edu*

James Wiegold
School of Mathematics, Cardiff University, Cardiff CF24 4Y, United Kingdom.
e-mail: *wiegoldj@cardiff.ac.uk*

Abstract: We prove that if p is a prime and W is the standard wreath product of two nontrivial cyclic p-groups X and Y then W is isomorphic to the full automorphism group of some group if and only if $|X| = 2$ and $|Y|$ is 2 or 4.

Keywords: automorphisms of groups, p-groups, wreath products.

Math. Subj. Classification (2000): 20F28, 20E36, 20D45.

In [2] we proved that the full automorphism group of a group is quite rarely isomorphic to a p-group of maximal class, where p is a prime—never, for instance, if $p > 3$. A special case of our theorem is that if p is an odd prime then $\operatorname{Aut} G$ cannot be isomorphic to the (standard) wreath product $\mathcal{C}_p \wr \mathcal{C}_p$ of two groups of order p, for any group G. This is false of course if $p = 2$, since $\mathcal{C}_2 \wr \mathcal{C}_2$, the dihedral group of order 8, is isomorphic to its own automorphism group.

Here we pursue the same kind of investigation with reference to more general wreath products, namely, for any prime p, wreath products of two nontrivial cyclic p-groups. As for the wreath products of two groups of order p it emerges that the groups that we consider are never isomorphic to the full automorphism group of any group if p is odd. Even for $p = 2$ we have that this happens in two cases only. Our main theorem is the following.

Theorem. *Let p be a prime, and let λ and μ be positive integers. Then there exists a group G such that $\operatorname{Aut} G \simeq \mathcal{C}_{p^\lambda} \wr \mathcal{C}_{p^\mu}$ if and only if $p^\lambda = 2$ and $p^\mu \in \{2, 4\}$.*

As is well-known, $\operatorname{Aut} G \simeq \mathcal{C}_2 \wr \mathcal{C}_2$ if and only if $G \simeq \mathcal{C}_2 \wr \mathcal{C}_2$ or $G \simeq \mathcal{C}_4 \times \mathcal{C}_2$; our proof will show that if $\operatorname{Aut} G \simeq \mathcal{C}_2 \wr \mathcal{C}_4$ then G is necessarily an infinite nilpotent group of class 3, with fairly restricted structure (see Proposition 3.10).

In contrast with this result we mention that for any prime p and any finite nontrivial group K, Heineken and Liebeck [6] (see Zureck [11] for the case $p = 2$, and also [5], [8], [10]) have constructed a finite p-group G of nilpotency class 2 such that $\operatorname{Aut} G$ is isomorphic to the wreath product of an abelian p-group of exponent p or 4 by K.

This research was begun while the first author was enjoying the excellent hospitality of the Mathematics Department of Bucknell University, partially supported by UPIMDS of Università Federico II, Napoli. He expresses his gratitude to both institutions.

1. Preparation

Much of our argument will involve describing certain normal subgroups of the automorphism group $\operatorname{Aut} G$ of a group G under the hypothesis that $\operatorname{Aut} G$ be decomposable as a wreath product of two nontrivial cyclic p-groups. We shall be mainly concerned with the group of inner automorphisms $\operatorname{Inn} G$, its centralizer $\operatorname{Aut}_c G$, that is, the group of central automorphisms of G, and with centralizers in $\operatorname{Aut} G$ of other characteristic subgroups and quotients of G. Thus it seems convenient to collect here some elementary facts about the normal structure of such wreath products.

For the lemmas in this section we fix the following notation: p is a prime, $\lambda, \mu \in \mathbb{N}$ and $A = \langle\beta\rangle \wr \langle\alpha\rangle$, where β and α have orders p^λ and p^μ respectively. Furthermore, $B = \langle\beta\rangle^A$ is the base subgroup of A.

Lemma 1.1. *Let Γ be a normal subgroup of A not contained in B. Suppose that either of p^λ and $|\Gamma B/B|$ is greater than 2. Then $C_A(\Gamma)$ is a subgroup of B of rank $|A/\Gamma B|$.*

Proof — Let $\gamma \in \Gamma \smallsetminus B$. If $p^\lambda = 2$ choose γ such that $\gamma^2 \notin B$. Then no nontrivial power of α commutes with $[\beta,\gamma]$, which belongs to Γ. Hence $C_A(\Gamma) \le C_A\big([\beta,\gamma]\big) = B$. Now, let $q = |A/\Gamma B|$. Then B can be decomposed as a direct product of $\langle\alpha^q\rangle$-invariant subgroups: $B = \operatorname{Dr}_{i=0}^{q-1} B_i$, where $B_i = \langle\beta^{\alpha^i}\rangle^{\langle\alpha^q\rangle}$ for each i. Also, for each i, the subgroup $B_i\langle\alpha^q\rangle$ is isomorphic to the wreath product $\langle\beta\rangle \wr \langle\alpha^q\rangle$. Therefore $C_{B_i}(\Gamma) = C_{B_i}(\alpha^q)$ is cyclic (of order p^λ) for each i, and $C_A(\Gamma) = \operatorname{Dr}_{i=0}^{q-1} C_{B_i}(\Gamma)$ has rank q. □

Lemma 1.2. *Let Γ be a normal abelian subgroup of A not contained in B. Then $p^\lambda = 2$ and $\Gamma = C_A(\Gamma) = [B,\alpha_0]\langle\gamma\rangle \le B\langle\alpha_0\rangle$ for some $\gamma \in \Gamma \smallsetminus B$, where α_0 is the element of order 2 in $\langle\alpha\rangle$, and $B \cap \Gamma = [B,\alpha_0]$.*

Proof — Lemma 1.1 shows that $p^\lambda = 2 = |\Gamma B/B|$. Hence $\Gamma = (B\cap\Gamma)\langle\gamma\rangle$, for some $\gamma \in B\alpha_0$. Since $B\cap\Gamma \ge [B,\gamma] = [B,\alpha_0] = C_B(\alpha_0) = C_B(\gamma) \ge B\cap\Gamma$ we have that $B\cap\Gamma = [B,\alpha_0] = C_B(\gamma)$. Now, $C_A([B,\alpha_0]) = B\langle\alpha_0\rangle = B\langle\gamma\rangle$, so that $\Gamma = C_A(\Gamma)$. □

Lemma 1.3. *Let q be a proper factor of p^μ and let D be a subgroup of B such that $[B,\alpha^q] \le D$. Then $\operatorname{rk}\big(D/[D,\alpha^q]\big) \ge q$. Moreover, if $\operatorname{rk}\big(D/[D,\alpha^q]\big) = q$ then D is a direct factor of B.*

Proof — As in the proof for Lemma 1.1 we can write $B = \operatorname{Dr}_{i=0}^{q-1} B_i$, where $B_i = \langle\beta^{\alpha^i}\rangle^{\langle\alpha^q\rangle}$ for each i. Let $\bar D = D/D^p$. Then α^q acts on $\bar D$ and the mapping given by $x \mapsto [x,\alpha^q]$ is an endomorphism of $\bar D$, thus $\bar D/C_{\bar D}(\alpha^q) \simeq [\bar D,\alpha^q]$. It follows that $\big|\bar D/[\bar D,\alpha^q]\big| = |C_{\bar D}(\alpha^q)|$. Now $\big|D/D^p[D,\alpha^q]\big| = \big|\bar D/[\bar D,\alpha^q]\big|$, hence, to prove that $\operatorname{rk}\big(D/[D,\alpha^q]\big) \ge q$, what we have to show is that $|C_{\bar D}(\alpha^q)| \ge p^q$.

Since $[B,\alpha^q] \le D$ we have that $[B^p,\alpha^q] = [B,\alpha^q]^p \le D^p$. Then $C_{\bar D}(\alpha^q)$ contains $(B^pC_B(\alpha^q)\cap D)/D^p$. Let $t = p^\mu/q$, the order of α^q. Also let $c_0 = \beta\beta^{\alpha^q}\beta^{\alpha^{2q}}\cdots\beta^{\alpha^{(t-1)q}}$, a generator of $C_{B_0}(\alpha^q)$, and $x_0 = \beta^{-t}c_0$. Then $x_0 = \prod_{i=0}^{t-1}[\beta,\alpha^{iq}] \in [B_0,\alpha^q]$. Next, for every $i \in \{1,2,\dots,q-1\}$, let $x_i = x_0^{\alpha^i}$. Then $x_i \in [B_i,\alpha^q] \le B_i \cap D$ and $x_i \in B^pC_B(\alpha^q)$, hence $x_iD^p \in C_{\bar D}(\alpha^q)$ for all $i \in \{0,1,\dots,q-1\}$. Also, the elements x_i are clearly independent modulo B^p, hence modulo D^p. Therefore, if $H := \langle x_0,\dots,x_{q-1}\rangle$, then HD^p/D^p has order p^q and is contained in $C_{\bar D}(\alpha^q)$. Thus $\operatorname{rk}\big(D/[D,\alpha^q]\big) \ge q$. Also note that since HB^p/B^p has order p^q as well, we have $B^p \cap H \le D^p$.

Finally, suppose that the rank of $D/[D,\alpha^q]$ is exactly q. Then $HD^p/D^p = C_{\bar D}(\alpha^q)$. Since $(B^p\cap D)/D^p \le C_{\bar D}(\alpha^q)$ we get $B^p \cap D = B^p \cap HD^p = (B^p\cap H)D^p = D^p$. Since B is homocyclic, therefore D is a pure subgroup of B, hence a direct factor. □

Lemma 1.4. *Let Γ be a normal subgroup of A not contained in B. Suppose that either of p^λ and $|\Gamma B/B|$ is greater than 2. Then Γ cannot be generated by $|A/\Gamma B|$ elements.*

Proof — Let $q = |A/\Gamma B|$. There exists $\xi \in B$ such that $\Gamma = D\langle\gamma\rangle$, where $D = \Gamma \cap B$ and $\gamma = \alpha^q\xi$— of course, ξ is only determined modulo D. Then D contains $[B,\gamma] = [B,\alpha^q]$, thus satisfying the hypothesis of Lemma 1.3. Let F be the Frattini subgroup of Γ. Then $\Gamma/F = \langle\gamma F\rangle \times DF/F$. Since $\langle\gamma F\rangle \ne 1$, it will be enough to prove that DF/F has rank at least q. Set $D^* = D^p[D,\alpha^q]$, so that

$F = D^*\langle\gamma^p\rangle$. The group DF/F is an epimorphic image of D/D^*: the latter is an extension of the cyclic group $F \cap D/D^*$ by $D/F \cap D \simeq DF/F$. Hence $\mathrm{rk}(DF/F) = \mathrm{rk}(D/D^*) - \mathrm{rk}(F \cap D/D^*) \geq \mathrm{rk}(D/D^*) - 1$. Thus what we have to prove is that either $\mathrm{rk}(D/D^*) > q$ or $\mathrm{rk}(D/D^*) = q$ and $F \cap D = D^*$. We have $\mathrm{rk}(D/D^*) \geq q$ by Lemma 1.3, so we may assume that $\mathrm{rk}(D/D^*) = q$. Then, by the same lemma, $B = D \times E$ for some E. We can redefine γ in such a way that $\xi \in E$. We have to prove that $F \cap D = D^*$, that is, $\langle\gamma^p\rangle \cap D \leq D^*$. Now, $\langle\gamma^p\rangle \cap D = \langle\gamma\rangle \cap D = \langle\gamma^t\rangle$, where $t = p^\mu/q = |\Gamma B/B|$. Let us compute γ^t modulo D^*. Since $[\alpha^q, \xi]$ lies in D and so commutes with α^q modulo D^*, it follows that $\gamma^t \equiv \alpha^{qt}\xi^t[\xi, \alpha^q]^{t(t-1)/2} \pmod{D^*}$. Now, $\alpha^{qt} = \alpha^{p^\mu} = 1$. Since $\gamma^t, [\xi, \alpha^q] \in D$ it also follows that $\xi^t \in D$, but $\xi \in E$, and so $\xi^t = 1$. Therefore $\gamma^t \equiv [\xi, \alpha^q]^{t(t-1)/2} \pmod{D^*}$. If $t > 2$ then p divides $t(t-1)/2$, hence $[\xi, \alpha^q]^{t(t-1)/2} \in D^p \leq D^*$ and $\gamma^t \in D^*$. If $t = 2$ then $\xi^2 = 1$, but $\exp B = 2^\lambda > 2$ by hypothesis, so $\xi \in B^2$. Hence $[\xi, \alpha^q] \in [B^2, \alpha^q] = [B, \alpha^q]^2 \leq D^2 \leq D^*$. Therefore $\gamma^t \in D^*$ in this case as well, as we wanted to show. □

Another important property of the normal subgroups of A that we will make use of is that, in the above notation, the normal subgroups of A contained in the socle of B are totally ordered by inclusion (see [9], Lemma 6.2.4 for instance).

Finally, for ease of reference we record three elementary and certainly well-known remarks, whose proofs are omitted:

Lemma 1.5. *If $\lambda \leq \mu$ then $Z(A) \leq A'$.*

Lemma 1.6. *Let G be a nilpotent group of class 2 and let X be a subgroup such that $Z(G) \leq X \leq G$ and G/X is cyclic. Then $\exp\big(G/Z(G)\big) = \exp\big(X/Z(G)\big)$.*

Lemma 1.7. *Let G be a group such that $|G/G^2| = 8$ and $|G'| = 2$. Then $|G/Z(G)| = 4$.*

2. An example

In this section we shall construct a group G such that $\mathrm{Aut}\, G \simeq \mathcal{C}_2 \wr \mathcal{C}_4$. The results in the next section will show that all groups having this property share much of their structure with this example.

Let us start with the group G_0 defined as follows:

$$G_0 = \big(\langle c, z\rangle \rtimes \langle a\rangle\big) \rtimes \langle b\rangle,$$

where $\langle c, z\rangle$ is isomorphic to V_4, the noncyclic group of order 4, both a and b have infinite order, $c = [a, b]$ and $z = [c, a] = [c, b] \in Z(G_0)$. Thus $G_0' = \langle c, z\rangle \simeq V_4$ and G_0/G_0' is free abelian on aG_0' and bG_0'. Also, G_0 is nilpotent of class 3 and $\gamma_3(G_0) = \langle z\rangle$. Therefore the next lemma may be applied to G_0.

Lemma 2.1. *Let G be a nilpotent group of class 3 such that G' has exponent 2. Then $G^4 \leq Z(G)$ and the mapping $g \in G \mapsto g^4 \in G^4$ is an epimorphism. Furthermore G^2 is abelian and $[G^2, G] \leq \gamma_3(G)$.*

Proof — Let $K = \gamma_3(G)$. Then $\bar{G} = G/K$ is a class-2 nilpotent group whose derived subgroup has exponent 2, hence $\bar{G}^2 \leq Z(\bar{G})$. Thus $[G^2, G] \leq K$, in particular $G^2 \leq Z_2(G)$. It follows that $[G^2, G^2] = [G^4, G] = [G^2, G]^2 \leq K^2 = 1$, hence G^2 is abelian and $G^4 \leq Z(G)$. Next, for every $x, y \in G$, we have $(xy)^2 = x^2y^2[y, x][y, x, y]$ and so $(xy)^4 = x^4y^4$, because G' has exponent 2. □

It is easy to check that G_0 has an automorphism $\hat{\alpha}$ defined by:

$$a \longmapsto b \longmapsto a^{-1} \qquad \text{and, consequently,} \qquad c \longmapsto cz, \qquad z \longmapsto z.$$

Let $(p_i)_{i\in\mathbb{N}}$ be a family of primes congruent to 1 modulo 4 and such that $p_i \neq p_j$ if $i \neq j$. For every $i \in \mathbb{N}$ there exists $\lambda_i \in \mathbb{Z}$ such that $\lambda_i^2 \equiv -1 \pmod{p_i}$; choose such a λ_i and let $h_i = ab^{\lambda_i}$. Define recursively an ascending chain of groups as follows. For every $i \in \mathbb{N}$ let G_i be a central product $G_{i-1}\langle z_i\rangle$, where $\langle z_i\rangle$ is infinite cyclic, $h_i^{1-p_i} = z_i^{p_i}$ and $z_i \notin G_{i-1}$ (the latter condition being a consequence of the previous ones anyway), hence $|G_i/G_{i-1}| = p_i$. To check that these groups are well-defined, note that at each stage the hypotheses of Lemma 2.1 are satisfied by G_{i-1} and so $h_i^{1-p_i} \in G_0^4 \leq Z(G_{i-1})$. Define G as the direct limit of the groups G_i for i ranging over $\mathbb{N}_0$. We have that $G' = G_0'$ and G satisfies the hypotheses of Lemma 2.1. Moreover, G' is $\operatorname{tor} G$, the torsion subgroup of G. Indeed, G_0/G' is torsion-free and G/G_0 is periodic and has the subgroups $\langle z_i\rangle G_0/G_0$ as primary components, each of order p_i. If G/G' is not torsion-free then there exist some $i \in \mathbb{N}$ and some $g \in G_0$ such that gz_i is periodic. Hence $(gz_i)^{p_i} \in \operatorname{tor} G_0 = G'$. But $(gz_i)^{p_i} = g^{p_i}h_i^{1-p_i}$, thus $h_i \in G_0'G_0^{p_i}$, which is false. Therefore G/G' is torsion-free, as claimed.

We shall extend $\hat\alpha$ to an automorphism of G. To this end, note that for every $i \in \mathbb{N}$ we have $h_i = (h_iz_i)^{p_i}$ and, modulo $G_0'G_0^{p_i}$:

$$h_i^{\hat\alpha} = \bigl(ab^{\lambda_i}\bigr)^{\hat\alpha} \equiv a^{-\lambda_i}b \equiv \bigl(ab^{\lambda_i}\bigr)^{-\lambda_i} = h_i^{-\lambda_i} \in G_i^{p_i},$$

hence $h_i^{\hat\alpha} \in G_0'G_i^{p_i} = G_i^{p_i}$, since G_0' has order 4 and p_i is odd the former is contained in $G_i^{p_i}$. Thus $z_i^{p_i\hat\alpha} = (h_i^{\hat\alpha})^{1-p_i} \in G_i^{p_i}$.

The fact that the mapping given by $x \mapsto x^4$ is an endomorphism of G_i whose image is contained in $Z(G_i)$ implies that the mapping given by $x \mapsto x^{p_i}$ is an epimorphism from G_i to $G_i^{p_i}$—an isomorphism actually, since $\operatorname{tor} G_i = G'$ has order 4; it is relevant here that $p_i \equiv 1 \pmod 4$. Thus there exists $r_i \in G_i$ such that $r_i^{p_i} = z_i^{p_i\hat\alpha}$. Since $p_i \equiv 1 \pmod 4$ and $G_i^4 \leq Z(G_i)$ we have that $r_i \in Z(G_i)$; also $r_i \notin G_{i-1}$, because $r_i^{p_i} = (h_i^{\hat\alpha})^{1-p_i} \notin G_0^{p_i}$ and p_i does not divide $|G_{i-1}/G_0|$, and this makes clear that, as claimed, $\hat\alpha$ can be extended to an automorphism α of G by mapping each z_i to r_i.

To simplify the argument it is perhaps useful to remark that the automorphisms of G are determined by their actions on $\{a, b\}$. Indeed, $G = \langle a, b\rangle G^4$, hence if $\gamma \in \operatorname{Aut} G$ is such that $a^\gamma = a$ and $b^\gamma = b$ then γ acts trivially on G/G^4. On the other hand, G_{ab} is torsion-free and has $\{aG', bG'\}$ as a maximal independent subset, hence γ acts trivially on G_{ab} too. Now, G' is the kernel of the epimorphism $x \in G \mapsto x^4 \in G^4$, hence $G^4 \simeq G/G'$ is torsion-free, therefore $G^4 \cap G' = 1$ and so $\gamma = 1$. This establishes our claim.

Since α^2 maps a and b to their inverses we have that α has order 4. For any $x \in G$ let $\tilde x$ be the inner automorphism of G determined by x. Let $\beta := \tilde a\alpha^2$; clearly $\beta \neq 1$. Also, $\beta^2 = \tilde a\alpha^2\tilde a\alpha^2 = \tilde a(\tilde a)^{\alpha^2} = \tilde a\widetilde{(a^{\alpha^2})} = \tilde a\widetilde{a^{-1}} = 1$, so β has order 2. Next, $\beta^\alpha = (\tilde a\alpha^2)^\alpha = \tilde a^\alpha\alpha^2 = \tilde b\alpha^2$, so that

$$\beta\beta^\alpha = \tilde a\alpha^2\tilde b\alpha^2 = \tilde a\tilde b^{\alpha^2} = \widetilde{ab^{-1}} \qquad\text{and}\qquad \beta^\alpha\beta = \tilde b\alpha^2\tilde a\alpha^2 = \tilde b\tilde a^{\alpha^2} = \widetilde{ba^{-1}} = \bigl(\widetilde{ab^{-1}}\bigr)^{-1}.$$

Now, ab^{-1} centralizes c, hence G', and so $[(ab^{-1})^2, G] = [ab^{-1}, G]^2 = 1$, because G' has exponent 2. Therefore $(ab^{-1})^2 \in Z(G)$, which proves that $\beta\beta^\alpha = \beta^\alpha\beta$. The next conjugate of β that we take into account is $\beta^{\alpha^2} = \alpha^2(\tilde a\alpha^2)\alpha^2 = \alpha^2\tilde a$. We have $\beta\beta^{\alpha^2} = \tilde a\alpha^2\alpha^2\tilde a = \tilde a^2$ and $\beta^{\alpha^2}\beta = \alpha^2\tilde a\tilde a\alpha^2 = (\tilde a^2)^{\alpha^2} = \tilde a^{-2}$. As $a^4 \in Z(G)$ then $\beta\beta^{\alpha^2} = \beta^{\alpha^2}\beta$. Therefore β commutes with both β^α and β^{α^2}. Since α has order 4 we have that $B := \langle\beta\rangle^{\langle\alpha\rangle}$ is (elementary) abelian (of rank at most 4). By our previous calculation $[\beta, \alpha] = \beta\beta^\alpha = \widetilde{ab^{-1}}$, and it follows that $[\beta, \alpha, \alpha^2]$ is the inner automorphism determined by $[a^{-1}, b]$, which is not trivial. Therefore α induces an automorphism of order 4 on $[B, \alpha]$, hence $\operatorname{rk}\bigl([B, \alpha]\bigr) \geq 3$ and $\operatorname{rk} B = 4$ (here, as elsewhere, $\operatorname{rk}(X)$ denotes the rank of the group X). This shows that $\langle\alpha, \beta\rangle$ is a subgroup of $\operatorname{Aut} G$ isomorphic to the wreath product $\mathcal{C}_2 \wr \mathcal{C}_4$. We shall prove that this subgroup is actually the whole of $\operatorname{Aut} G$. It will be enough to show that $|\operatorname{Aut} G| \leq 2^6$.

By considering $\{aG', bG', h_iz_iG' \mid i \in \mathbb{N}\}$ as a set of generators of G_{ab} it is immediately checked that G_{ab} is isomorphic to one of the groups in [4], p. 271, Example 1, whose automorphism groups are cyclic of order 4. Thus $\operatorname{Aut} G_{\mathrm{ab}} \simeq \mathcal{C}_4$. As $|G'| = 4$ and $\operatorname{Aut} G$ centralizes $\langle z\rangle = \gamma_3(G)$ it is clear that $\bigl|\operatorname{Aut} G/C_{\operatorname{Aut} G}(G')\bigr| \leq 2$. Hence it will suffice to show that $\mathit{\Gamma} := C_{\operatorname{Aut} G}(G') \cap C_{\operatorname{Aut} G}(G_{\mathrm{ab}})$ has order 8 at most. We know that $\mathit{\Gamma}$ is isomorphic to $D := \operatorname{Der}(G_{\mathrm{ab}}, G')$. Since the elements of $\mathit{\Gamma}$ are determined by their actions on a and b, by a remark above, the elements of D are determined by their actions on $\bar a := aG'$ and $\bar b := bG'$. Thus $|D| \leq |G'|^2 = 16$; it will be enough to show that not every mapping from $\{\bar a, \bar b\}$ to G' gives rise to a derivation. Let $\delta \in D$. From $\bar a\bar b = \bar b\bar a$ we obtain $(\bar a^\delta)^b\bar b^\delta = (\bar b^\delta)^a\bar a^\delta$, hence $\bar a^\delta[\bar a^\delta, b]\bar b^\delta = \bar b^\delta[\bar b^\delta, a]\bar a^\delta$ and so $[\bar a^\delta, b] = [\bar b^\delta, a]$. Since ab^{-1} centralizes G', and so $[\bar a^\delta, b] = [\bar a^\delta, a]$, this means that $\bar a^\delta$ and $\bar b^\delta$ must be congruent modulo $C_{G'}(a) = \langle z\rangle$. It follows that $|D| \leq 8$, as required. This proves that $\operatorname{Aut} G = \langle\alpha, \beta\rangle \simeq \mathcal{C}_2 \wr \mathcal{C}_4$.

3. Proof of the Theorem

We fix some notation and hypotheses that will hold throughout this section. Let p be a prime and λ, μ positive integers. We assume that G is a group whose automorphism group $A := \operatorname{Aut} G$ is isomorphic to the standard wreath product $\mathcal{C}_{p^\lambda} \wr \mathcal{C}_{p^\mu}$. Thus we can write $A = \langle \alpha, \beta \rangle = B \rtimes \langle \alpha \rangle$ for suitable automorphisms α, β of G, of orders p^μ and p^λ respectively, where $B = \mathrm{Dr}_{i=0}^{p^\mu - 1} \langle \beta \rangle^{\alpha^i}$ corresponds to the base subgroup of the wreath product $\langle \beta \rangle \wr \langle \alpha \rangle$. In agreement with notation in Section 1 we denote by α_0 an element of order p in $\langle \alpha \rangle$. We set $I := \operatorname{Inn} G$. Since we are not interested in the trivial case when A is dihedral we also stipulate that $A \not\simeq D_8$, that is to say, at least one of p^λ and p^μ is greater than 2.

We can apply to G results proved or quoted in Section 1 of [2] on every group whose automorphism group is a finite p-group.

In particular, the periodic elements of G form a finite subgroup T, which is a finite p-group if G is infinite, and still in this case G/T is a torsion-free abelian group whose automorphism group is finite and which therefore has finite quotients (modulo characteristic subgroups) of arbitrarily high exponent. By a theorem of Hallett and Hirsch (see [4], Theorem 116.1), $A/C_A(G/T)$ is a group of exponent at most 12. Since $\exp A = p^{\lambda+\mu}$ does not divide 12 it follows that $T \neq 1$.

As a further piece of notation, let $Z := Z(G)$ and $S := T \cap Z$; obviously G/Z also is a finite p-group and $S \neq 1$.

Since $Z(A)$ is cyclic A has a unique normal subgroup of order p, namely the socle $Z(A)[p]$ of $Z(A)$. We can then reproduce the argument in [2], Lemma 2.2 to show that G has exactly one characteristic subgroup of order p, say N, and exactly one characteristic subgroup of index p, which we will denote throughout by M, and that $Z(A)[p] = C_A(G/N) \cap C_A(M)$. Then we have:

Lemma 3.1. *$C_A(M)$ is a nontrivial cyclic subgroup of B.*

Proof — Both $C_A(M)$ and $C_A(G/N)$ are normal in A and abelian, because they stabilize the series $1 < M < G$ and $1 < N < G$ respectively. Since the A-invariant subgroups of the socle $B[p]$ of B form a chain and clearly $Z(A) \leq B$, we have $Z(A)[p] = C_{B[p]}(X)$ where X is either G/N or M, and $C_B(X)$ is cyclic. Moreover, if $C_A(X) \not\leq B$ then Lemma 1.2 shows that $\exp B = p^\lambda = 2$ and $C_B(X) = [B, \alpha_0]$, which is false because $C_B(X)$ is cyclic and $A \not\simeq D_8$. Thus $C_A(X) \leq B$. Finally, $C_A(G/N) \simeq \operatorname{Hom}(G/N, N)$ is not cyclic, since G/Z is not, hence $X = M$. □

By the arguments in Lemma 1.4 and Lemma 2.3 of [2] we also have:

Lemma 3.2. *M contains all proper characteristic subgroups of G whose index is finite and a power of p. Moreover, G is not abelian.*

Lemma 3.1 yields that $\operatorname{Hom}(G/M, S) \simeq C_A(G/S) \cap C_A(M)$ is cyclic. On the other hand this group is isomorphic to the socle of S. Therefore:

Lemma 3.3. *S is cyclic.*

Next we have two key lemmas on some normal subgroups of A. Recall that I denotes $\operatorname{Inn} G$.

Lemma 3.4. *$I \leq B\langle \alpha_0 \rangle$. If $p^\lambda > 2$ then $I \leq B \leq \operatorname{Aut}_c G$ and G has nilpotency class 2.*

Proof — The subgroup $C_A(G/S[p]) \cap C_A(Z)$ of $\operatorname{Aut}_c G$ is isomorphic to $\operatorname{Hom}(G/Z, S[p])$ and hence to the Frattini factor group $I/I'I^p$ of I. Thus $\operatorname{rk}(\operatorname{Aut}_c G) \geq d$, where d is the minimal number of generators of I. Suppose that $I \not\leq B$ and that either $|IB/B| > 2$ or $p^\lambda > 2$. Then $\operatorname{rk}(\operatorname{Aut}_c G) = |A/IB|$ by Lemma 1.1. On the other hand, Lemma 1.4 shows that $d > |A/IB|$, and this is a contradiction. Therefore $|IB/B| \leq 2$, hence $I \leq B\langle \alpha_0 \rangle$, and $I \leq B$ if $p^\lambda > 2$. In this latter case $\operatorname{Aut}_c G = C_A(I) \geq B$ and I is abelian; since G is not abelian (Lemma 3.2) we have that G has class 2. □

Lemma 3.5. *Suppose that G is infinite and $T \nleq Z$. Then $C_A(T) \cap C_A(G/T) \nleq \operatorname{Aut}_c G$ and $p^\lambda = 2$.*

Proof — Since $S < T$ there exists a characteristic subgroup R of T in which S is maximal, by Lemma 1.4 of [2]. Then $R \leq Z_2(G)$. As $|R/S| = p$ and S is cyclic we therefore have that $[R, G] = S[p]$ and so $\big|G/C_G(R)\big| = p$. But $C_G(R)$ is characteristic in G, thus $C_G(R) = M$ by Lemma 3.2. Let $r \in R \smallsetminus S$, and let p^t be the order of r. We claim that there exists $L \leq M$ such that $T \leq L$ and G/L is cyclic of order p^{t+1}. Indeed, $\bar{G} := G/TG^{p^{t+1}}$ is a finite abelian group of exponent p^{t+1}, by Lemma 1.3 of [2]. Let $\bar{M} = M/TG^{p^{t+1}}$. By Lemma 3.2 all elements of order at most p^t in $\bar{G}$ belong to $\bar{M}$. As $\bar{M}$ is maximal in $\bar{G}$ it easily follows that $\bar{G} = \langle a \rangle \times U$ for some element a of order p^{t+1} and some U such that $\bar{M} = \langle a^p \rangle \times U$. Define L as the preimage of U in G; all the required properties hold and the claim is established. Now let $x \in G$ be such that $G = L\langle x \rangle$. We can define an automorphism γ of G by mapping every element of L to itself and letting $x^\gamma = xr$. That γ is well-defined follows from the fact that $r \in Z(L)$ and that $(xr)^{p^{t+1}} = x^{p^{t+1}} r^{p^{t+1}} = x^{p^{t+1}}$; the latter equalities hold because $\langle x, r \rangle$ has nilpotency class 2 and commutator subgroup of order p. Now $[T, \gamma] = 1$ and $r \in [G, \gamma] \smallsetminus Z$, so that γ is not central, but it centralizes T and G/T. Thus $C_A(T) \cap C_A(G/T) \nleq \operatorname{Aut}_c G$.

Finally, assume that $p^\lambda > 2$. Since $C_A(T) \cap C_A(G/T)$ is abelian and normal in A, Lemma 1.2 shows that this subgroup is contained in B. On the other hand, by Lemma 3.4, we have $B \leq \operatorname{Aut}_c G$, and this contradicts what we have just proved. □

We are now in position to begin the actual proof of the theorem by examining which values of p, λ and μ may occur at all. We will first exclude the case that p is odd. The proof follows an argument from [2], proof of Theorem 2.11.

Lemma 3.6. $p = 2$.

Proof — Suppose that $p > 2$. If G is infinite then $T \leq Z$, by the previous lemma. But then G has an automorphism that centralizes T and acts like the inversion map on G/T ([2], Lemma 1.5); this automorphism has order 2, which is impossible. Thus G is finite. Since A has no nontrivial abelian direct factor it is easy to see that the p'-component of G has order at most 2 (see Lemma 2.1 of [2]) and we may assume that G is a p-group. By applying [7], Hilfssatz III.7.5 to $G \rtimes A$ we see that G has a noncyclic characteristic subgroup P of order p^2. By Lemma 3.2 then $P \leq M$. Let $\tilde{P}$ be the group of those inner automorphisms of G determined by elements of P. Then $\tilde{P} \lhd A$ and clearly $|\tilde{P}| \leq p$, hence $\tilde{P} \leq Z(A)[p] \leq C_A(M)$. Thus $P \leq Z(M)$. Now $C_A(M) = C_A(M) \cap C_A(G/M) \simeq \operatorname{Der}\big(G/M, Z(M)\big)$, and this derivation group is isomorphic to $K := \ker(1 + \sigma + \sigma^2 + \cdots + \sigma^{p-1})$, where σ is the automorphism of $Z(M)$ induced by conjugation by an element of $G \smallsetminus M$. It is straightforward to check that $P \leq K$, since σ induces on P an automorphism of order p at most. Hence P can be embedded in $C_A(M)$. This is a contradiction, because $C_A(M)$ is cyclic. □

Once it has been proved that $p = 2$ our previous lemmas suggest that we treat the cases $\lambda = 1$ and $\lambda > 1$ separately. Let us begin by disposing of the latter case.

Lemma 3.7. $\lambda = 1$.

Proof — Suppose that $\lambda > 1$. Then G has class 2, as shown in Lemma 3.4. Assume first that G is infinite. Then $T \leq Z$ by Lemma 3.5, and T is cyclic by Lemma 3.3. As T/G' is obviously a direct factor of G_{ab}, if $G' < T$ then $G = TK$ for some proper subgroup K of G such that $T \cap K = G'$. By Lemma 1.3 of [2] there exists an epimorphism $\varepsilon : K \twoheadrightarrow T$ (so $G' \leq \ker \varepsilon$). Since $T \leq Z$ we can construct two automorphisms of G as follows:

$$\gamma : \begin{cases} k \in K \mapsto k \\ t \in T \mapsto t^{1+|T|/2} \end{cases} \qquad \delta : \begin{cases} k \in K \mapsto kk^\varepsilon \\ t \in T \mapsto t \end{cases}.$$

Let N be the socle of T. Then γ belongs to $C_A(G/N) \cap C_A(N)$, which is abelian and normal in A and so is contained in B by Lemma 1.2; thus $\gamma \in B$. Similarly $\delta \in B$, because δ centralizes T and G/T. But it is easy to check that γ and δ do not commute. This is a contradiction, which proves that $G' = T$. Now consider $\Gamma := C_A(G/T)$. Since $T \leq Z$ we have $\Gamma \leq \operatorname{Aut}_c G$. As is well-known all central automorphisms act trivially on the derived subgroup, hence $\mathit{\Gamma}$ is the stabilizer of the series $1 < T < G$. Therefore $\mathit{\Gamma}$ is abelian, hence $\mathit{\Gamma} \leq B$, and $\mathit{\Gamma} \simeq \mathrm{Hom}(G/T, T)$. Also, by the theorem of Hallett and Hirsch already quoted, $\bar{A} := A/\mathit{\Gamma}$ is a group of exponent at most 4 in which all elements of order 2 lie in the centre. Since A is two-generator $|\bar{A}| \leq 32$ and $|\bar{A}'| \leq 2$, and $\bar{A}$ is even abelian if $\mu = 1$. As A' is homocyclic of rank $2^\mu - 1$ it follows that $A' \cap \mathit{\Gamma}$ has the same rank and exponent 2^λ. Therefore $\exp(G/Z) = |T| \geq \exp \mathrm{Hom}(G/T, T) \geq 2^\lambda > 2$. We use [2], Lemma 1.5 again to produce an automorphism φ of G of order 2 that centralizes T and acts like the inversion map on G/T. By what we have just proved $\varphi \notin \mathrm{Aut}_c G$, hence $\varphi \notin B$ by Lemma 3.4. It is immediate to check that the socle $\mathit{\Gamma}[2]$ of $\mathit{\Gamma}$ is $C_A(G/G^2) \cap C_A(N) \simeq \mathrm{Hom}(G/G^2, N) \simeq G/G^2$ and centralizes φ. By Lemma 1.1 it follows that $\mathrm{rk}(G/G^2) = \mathrm{rk}(\mathit{\Gamma}) \leq |A/B\langle\varphi\rangle| = 2^{\mu-1}$. We have already shown that $\mathrm{rk}(\mathit{\Gamma}) \geq \mathrm{rk}(A' \cap \mathit{\Gamma}) = 2^\mu - 1$, hence $\mu = 1$. Thus G/G^2 is cyclic, but this is a contradiction because G/Z is not cyclic.

Therefore G is finite. Let Σ be the centralizer in A of Z and G/Z. Then $\Sigma \simeq \mathrm{Hom}(G/Z, Z) \simeq G/Z \simeq I$, because Z is cyclic and $G' \leq Z$, so $\exp(G/Z) = |G'| \leq |Z|$. On the other hand $I \leq \Sigma$, so $I = \Sigma$. It follows that $A' \leq I$, because $A' \leq B \leq \mathrm{Aut}_c G$ by Lemma 3.4, hence A' centralizes G/Z, and A' centralizes Z as well, as Z is cyclic. Thus $A' \leq I \leq B$; since $C_A(A') = B$ it follows that $\mathrm{Aut}_c G = B$. Also, $|G'| = \exp I = 2^\lambda$. Now G has no nontrivial abelian direct factor, because Z is cyclic. By a theorem of Adney and Yen [1] it follows that $|\mathrm{Aut}_c G| = \big|\mathrm{Hom}(G, Z)\big|$. But $\exp G_{\mathrm{ab}} \leq \exp(G/Z) \cdot |Z/G'| = |G'| \cdot |Z/G'| = |Z|$, hence $\mathrm{Hom}(G, Z) \simeq \mathrm{Hom}(G_{\mathrm{ab}}, Z) \simeq G_{\mathrm{ab}}$. Thus the above equality becomes $|B| = |G_{\mathrm{ab}}|$. By the main theorem in [3] we have that $|G| \leq |A|$; since $|G| = |G'| \cdot |G_{\mathrm{ab}}| = 2^\lambda |B|$ and $|A| = 2^\mu |B|$ we deduce that $\lambda \leq \mu$. Hence $Z(A) \leq A'$ by Lemma 1.5. This can be used to bound the size of Z. Indeed, the mapping $\theta : g \in G \mapsto g^{1+2^{\lambda+1}} \in G$ is an automorphism, hence it lies in $Z(A)$ and therefore in A'. But $A' \leq I$, hence θ centralizes Z, so $|Z| \leq 2^{\lambda+1}$. As $|G'| = 2^\lambda$ and $|B| = |G_{\mathrm{ab}}| = |I| \cdot |Z/G'|$ we get that $|B : I| \leq 2$. Since $\lambda > 1$ this implies that $\mathrm{rk}(G/Z) = \mathrm{rk}(I) = \mathrm{rk}(B) = 2^\mu$. Now let u be any element of $G \smallsetminus M$. The A-orbit of u generates a characteristic subgroup of G which is not contained in M, hence is G itself. Thus, by the last remark, this orbit must contain 2^μ elements which are independent modulo ZG^2. Since $B = \mathrm{Aut}_c G$ centralizes u modulo ZG^2 and $|A : B| = 2^\mu$ it follows that B is the centralizer in A of u modulo ZG^2. So, to reach a contradiction it will be enough to find such a u and a noncentral automorphism of G that fixes u modulo G^2. To this end, note first that the set of all elements $g \in G$ such that $[g, G] \leq (G')^2$ is a proper characteristic subgroup of G, so it is contained in M. Hence, if we choose any $u \in G \smallsetminus M$ we can find $v \in G$ such that $G' = \big\langle [u, v] \big\rangle$. We may clearly choose $v \notin M$: if $v \in M$ we simply replace it by uv. At the expense of interchanging u and v if needed, we may also assume that the order of u is not smaller than that of v. Then u^{2^λ} and v^{2^λ} both belong to Z, which is cyclic, hence $v^{2^\lambda} = u^{t2^\lambda}$ for some integer t. Let $w = u^{-t}v$. Then $w^{2^{\lambda+1}} = 1$ and $[u, w] = [u, v]$. Let $u_1 := uw^2$. Then $u_1^{2^\lambda} = u^{2^\lambda} w^{2^{\lambda+1}} [w, u]^{2^\lambda(2^\lambda - 1)} = u^{2^\lambda}$, because $|G'| = 2^\lambda$. As $[u, w] = [u_1, w]$ has order $2^\lambda = \exp(G/Z)$, we have that $\langle u \rangle \cap \langle w \rangle Z = \langle u^{2^\lambda} \rangle = \langle u_1 \rangle \cap \langle w \rangle Z$. This shows that there exists an automorphism of $H := \langle u, w \rangle Z$ which centralizes Z and w, and maps u to u_1. Now let $C := C_G(H) = C_G(\{u, w\})$. Then $|G : C| \leq 2^{2\lambda}$. On the other hand, u and w are independent modulo $Z(H)$, so $\big|H/Z(H)\big| = 2^{2\lambda}$. It follows that G is factorized as a central product HC; also $H \cap C = Z(H) = Z$ and so the above automorphism of H can be extended to an automorphism ψ of G acting trivially on C. It is clear that ψ is not central, since $[w^2, u] \neq 1$ and so $w^2 \notin Z$, but it fixes u modulo G^2. This contradiction completes the proof. $\square$

Therefore $p^\lambda = 2$, so we have identified the first factor of the wreath products that we are dealing with. Since we have excluded the case where A is isomorphic to D_8 we also have $\mu > 1$. Moreover, Lemma 3.1 now gives that $|C_A(M)| = 2$ and so $C_A(M) = Z(A)$. Furthermore, this also implies that $C_A(M) \leq I$, hence $C_G(M)/Z \simeq C_A(M)$. As $C_G(M) \leq M$ by Lemma 3.2, then $C_G(M) = Z(M)$ and $|Z(M)/Z| = 2$.

It is also relevant that the Hallett-Hirsch Theorem now gives stronger information, in the case that G is infinite. Indeed, as we already mentioned, this theorem implies that all elements of order 2 in $\bar{A} = A/C_A(G/T)$ are central; since B has exponent 2 this means that $\bar{A}$ is abelian, hence A'

centralizes G/T.

Lemma 3.4 shows that $I \leq B\langle\alpha_0\rangle$, which has class 2. Hence G has nilpotency class 3 at most. Let us see that the class is exactly 3.

Lemma 3.8. *G has nilpotency class* 3.

Proof — Suppose that G has class 2. Then I is an abelian subgroup of $B\langle\alpha_0\rangle$ and so is (elementary abelian)-by-cyclic. By Lemma 1.6 then $\exp(G/Z) = 2$. Now, G' is contained in S and hence is cyclic (Lemma 3.3). Thus $|G'| = 2$.

Suppose that G is finite. Then the mapping $\theta : g \in G \mapsto g^5 \in G$ is an automorphism. Hence $\theta \in Z(A)$. Thus $M^4 = [M, \theta] = 1$. Therefore Z, which is a cyclic subgroup of M, has order 4 at most. If M is abelian then $|M/Z| = |Z(M)/Z| = 2$, hence $|M| \leq 8$ and $|G| \leq 16$. Either M is cyclic or Z has a complement in M, so either $|M| \leq 4$ or $M \simeq \mathcal{C}_4 \times \mathcal{C}_2$. In any case $|\mathrm{Aut}\, M| \leq 8$. Since $C_A(M) = Z(A)$ has order 2 it follows that $|A| \leq 16$. But $|A| = 2^{2^\mu + \mu} \geq 2^6$, a contradiction. Therefore M is not abelian. Let u, $v \in M$ be such that $[u, v] \neq 1$, and let $H = \langle u, v\rangle$. Then $u^4 = v^4 = 1$ because M has exponent 4, and both u^2 and v^2 belong to the socle G' of Z. So $|H| = 8$. Also, G is the central product HC, where $C = C_G(H)$. If $H \simeq Q_8$ then H has an automorphism of order 3, which can be extended to G by letting it act trivially on C. This is a contradiction, hence $H \simeq D_8$. We may assume that u has order 4, hence $v^2 = 1$. If C has an element c of order 4 then $H_1 := \langle u, vc\rangle \simeq Q_8$ and we get a contradiction as above. Thus $\exp C = 2$. So C is abelian, hence $C \leq Z$. But then $C \leq H$ and $G = H$, a contradiction again. This proves that G cannot be finite.

Suppose then that G is infinite. Clearly G_{ab} splits over T/G', hence there exists a subgroup $V \leq G$ such that $TV = G$ and $V \cap T = G'$. Lemma 1.5 of [2] shows that V has an automorphism acting like the inverting map on V/G'. Since $V^2 \leq Z$ this can be exended to an automorphism φ of G centralizing T. Note that $[G, \varphi] \leq G^2 \leq Z$. Thus we have:

$$\varphi \in C_A(T) \cap \mathrm{Aut}_c\, G \smallsetminus C_A(G/T).$$

Assume that $G' = T$. Let $\Gamma = C_A(G/T)$. By the Hallett-Hirsch Theorem A/Γ is an abelian group of exponent at most 4, hence $A'A^4 = [B, \alpha]\langle\alpha^4\rangle \leq \Gamma$. On the other hand Γ is abelian, since $|T| = 2$ and so $[\Gamma, T] = 1$, actually $\Gamma \simeq \mathrm{Hom}(G/T, T) \simeq G/G^2$. Thus $\Gamma \leq C_A(A') = B$. Hence $\alpha^4 \in \langle\alpha\rangle \cap B = 1$ and so $\mu = 2$. It is easy to see that $[\varphi, \Gamma] = 1$, because φ centralizes G/G^2 and T, hence $\varphi \in B$. Then we have $A' \leq \Gamma \leq B$ and $\varphi \in B \smallsetminus \Gamma$; as $A' \lessdot B$ it follows that $\Gamma = A'$ (we use the symbol '$\lessdot$' for 'is a maximal subgroup of'). Therefore $G/G^2 \simeq \Gamma$ has rank 3, thus $|G/Z| = 4$ by Lemma 1.7. Hence I is $[B, \alpha^2]$, the only A-invariant subgroup of B of order 4, so that $\mathrm{Aut}_c\, G = B\langle\alpha^2\rangle$. Also, $I \leq C_A(G/Z) \cap C_A(Z) \simeq \mathrm{Hom}(G/Z, T) \simeq G/Z \simeq I$, so $I = C_A(G/Z) \cap C_A(Z)$. Therefore $[\Gamma, Z] \neq 1$, because $I < \Gamma$; we shall see that this leads to a contradiction. Let φ^* and α^* be the automorphisms induced on Z by φ and α respectively. It is clear that $\varphi^* = -1 + \varepsilon$, where ε is an endomorphism of Z such that $\mathrm{im}\, \varepsilon \leq T$. For every $x \in G$ we have $xx^\varphi \in T$, hence $x^{2\varphi} = \big(x^{-1}(xx^\varphi)\big)^2 = x^{-2}$. Thus $G^2 \leq \ker \varepsilon$. As $G^2 \lessdot Z$ then α acts trivially on $Z/\ker\varepsilon$, and likewise on $\mathrm{im}\,\varepsilon$, obviously. It follows that α^* commutes with ε and hence with φ^*. Therefore $[\varphi, \alpha] \in C_A(Z)$. But $\Gamma = A' = \langle[\varphi, \alpha]\rangle^A$, hence we obtain that $[\Gamma, Z] = 1$, the expected contradiction. Therefore $G' < T$.

Since G/T has quotients of arbitrary finite exponent ([2], Lemma 1.3) and S is cyclic the exponent of $\Sigma := C_A(G/S) \cap C_A(S) \simeq \mathrm{Hom}(G/S, S)$ is $|S|$. Also note that $I \leq \Sigma \leq \mathrm{Aut}_c\, G$ and $\Sigma \leq B\langle\alpha_0\rangle$ by Lemma 1.2, hence $|S| \leq 4$. We claim that $S \neq T$. Indeed, if $S = T$ then $|S| = 4$ because $G' < T$, and Σ has exponent 4. Since Σ has an elementary abelian subgroup of index 2 we have that $|\Sigma^2| = 2$. Moreover $Q := G/S$ is torsion-free, and $\Sigma \simeq \mathrm{Hom}(Q, S) \simeq Q/Q^4$, whence $|Q^2/Q^4| = 2$ and so $|Q/Q^2| = 2$. This means that $SG^2 \lessdot G$, which is impossible, as it would imply that G is abelian. Thus our claim is proved, therefore $T \not\leq Z$. As a consequence, by Lemma 3.5:

$$\Gamma := C_A(G/T) \cap C_A(T) \not\leq \mathrm{Aut}_c\, G.$$

If $I \not\leq B$ then Lemma 1.2 shows that $I = C_A(I) = \mathrm{Aut}_c\, G$. However the automorphism φ considered above is central but is certainly outer, since it does not centralize G/T. By this contradiction $I \leq B$

and consequently $B \leq \operatorname{Aut}_c G$. Now $\Gamma \leq B\langle\alpha_0\rangle$, because Γ is abelian, so as $\Gamma \nleq \operatorname{Aut}_c G$ it follows that $\operatorname{Aut}_c G = B$. Moreover, A' centralizes G/T by the Hallett-Hirsch Theorem, hence $\varphi \in B \setminus A'$ and so $B = \langle\varphi\rangle^A$. Since $\varphi \in C_A(T) \lhd A$ this shows that $[B, T] = 1$. But this is impossible, as $I \leq B$ and $T \nleq Z$. □

Lemma 3.9. $I = A'\langle\beta\alpha_0\rangle$. *Moreover:*

(*i*) *the set of all characteristic subgroups of* G *containing* Z *is totally ordered by inclusion;*

(*ii*) $M^2 \leq Z$*;*

(*iii*) $|S| = 2$*;*

(*iv*) ZG' *is a maximal subgroup of* $G^2 = Z_2(G)$ *and* $G^2/Z \simeq G/G^2$ *has rank* $2^{\mu-1}$. *Also,* G^2 *is abelian.*

Proof — From Lemma 3.4 we know that $I \leq B\langle\alpha_0\rangle$. Since I is not abelian, by Lemma 3.8, we have that $I = (I \cap B)\langle\gamma\rangle$, where $\gamma \in I \setminus B$ and $[I \cap B, \gamma] \neq 1$. Also, it is clear that $C_B(\gamma) = C_B(\alpha_0) = [B, \alpha_0] = [B, \gamma] \leq I$, because $I \lhd A$, and that $C_A(I \cap B) = B$ because γ does not centralize $I \cap B$, thus

$$\operatorname{Aut}_c G = C_A(I) = Z(I) = [B, \alpha_0] < I \cap B. \qquad (\star)$$

Besides proving statements (*i*)–(*iv*) we shall check that $I \cap B = A'$ and that $\beta\alpha_0 \in I$, thus making $\beta\alpha_0$ a suitable choice for γ.

The natural conjugation epimorphism $\sim: G \twoheadrightarrow I$ gives rise to the bijection $X \mapsto \widetilde{X}$—an isomorphism from the lattice of the characteristic subgroups of G containing Z to that of the A-invariant subgroups of I. As we mentioned in Section 1, the A-invariant subgroups of B (which equals its socle) form a chain. Now $I \cap B \lhd A$ and $|I/I \cap B| = 2$, hence Lemma 3.2 yields $I \cap B = \widetilde{M}$ and (*i*). Since $M/Z \simeq \widetilde{M}$, we also get (*ii*) as an immediate consequence. Let $J := \langle \gamma \in I \setminus B \mid \gamma^2 = 1\rangle$. For every $\eta \in B$ we have $(\eta\alpha_0)^2 = [\eta, \alpha_0]$, and this shows that all given generators of J lie in $C_B(\alpha_0)\alpha_0$, thus $J \leq C_B(\alpha_0)\langle\alpha_0\rangle$, which is abelian. Since I is not abelian it follows that $J < I$. But then (*i*) shows that $J \leq I \cap B = \widetilde{M}$, which means that $J = 1$. Hence every element of $I \setminus B$ has order 4, in particular, $\alpha_0 \notin I$. Fix $\gamma \in I \setminus B$. Then $\gamma = \sigma\alpha_0$ for some $\sigma \in B \setminus I$. Thus $I \cap B < B$; as $A' \lessdot B$ the total ordering property gives that $I \cap B \leq A'$. The mapping $f : \eta \in B \mapsto [\eta, \alpha_0] \in B$ is a homomorphism with kernel $[B, \alpha_0] \leq I \cap B$. Since $\sigma \notin I \cap B$ we have that $\sigma^f \notin (I \cap B)^f = [I \cap B, \alpha_0]$. But $\sigma^f = [\sigma, \alpha_0] = \gamma^2$ and $[I \cap B, \alpha_0] = [I \cap B, \gamma] = I'$, hence $\gamma^2 \notin I'$. This shows that $G/ZG' \simeq I/I'$ has exponent 4. Now $\operatorname{Aut}_c G = [B, \alpha_0]$ has exponent 2, hence the same holds for its subgroup $C_A(G/S) \cap C_A(S) \simeq \operatorname{Hom}(G/S, S)$. As $\exp(G/ZG') > 2$ it now follows that $\exp S = 2$. Since S is cyclic, $|S| = 2$, and so (*iii*) is proved. Now, $S < G'$, because G has class 3, hence there exists a characteristic subgroup V of G of order 4 contained in G' (see [2], Lemma 1.4). As $S < V$ then $I \nleq C_A(V)$ and $|A/C_A(V)| = 2$. Hence $I \nleq A^2 = A'\langle\alpha^2\rangle$, so that $\gamma \notin A'\langle\alpha^2\rangle$. Since $\alpha_0 \in \langle\alpha^2\rangle$ we deduce that $\sigma \notin A'$. But then $A' = [B, \alpha] = [\sigma, \langle\alpha\rangle] = [\gamma, \langle\alpha\rangle] \leq I$ and so $I \cap B = A'$. Now $\sigma \in B \setminus A' = A'\beta$, hence we have that $I = A'\langle\beta\alpha_0\rangle$, as required.

It remains to prove (*iv*). Firstly, $Z_2(G)/Z \simeq Z(I)$, and we know from ($\star$) that the latter is also equal to $\operatorname{Aut}_c G = [B, \alpha_0]$, an elementary abelian group of rank $2^{\mu-1}$. Next, the fact that $\operatorname{Aut}_c G \leq I$ shows that $\operatorname{Aut}_c G$ actually is the stabilizer of the series $1 < Z < G$, hence it is isomorphic to $\operatorname{Hom}(G/Z, Z) \simeq \operatorname{Hom}(G/Z, S) \simeq G/ZG^2$. On the other hand one subgroup of $\operatorname{Aut}_c G$ is $C_A(G/S) \simeq \operatorname{Hom}(G/S, S) \simeq G/G^2$. By comparing orders we therefore have $\operatorname{Aut}_c G = C_A(G/S)$ and $Z \leq G^2$. Further, $ZG'/Z \simeq I' = [A', \alpha_0]$, a maximal subgroup of $[B, \alpha_0]$, hence $ZG' \lessdot Z_2(G)$; moreover $I^2 = I'\langle\gamma^2\rangle$, where $\gamma = \beta\alpha_0$, and $\gamma^2 \notin I'$, hence $|I^2| = \big|[B, \alpha_0]\big|$ and so $I^2 = [B, \alpha_0]$ by (*i*). This proves that $G^2 = Z_2(G)$. Finally, since G' is central in $Z_2(G)$ it is now clear that G^2 is abelian.□

We can now complete the proof of the Theorem. It will be obtained by the example constructed in Section 2 and the next proposition, that sums up the content of this section.

Proposition 3.10. *Let p be a prime and let G be a group such that $\operatorname{Aut} G \simeq \mathcal{C}_{p^\lambda} \wr \mathcal{C}_{p^\mu}$ for some positive integers λ and μ. Then $p^\lambda = 2$ and μ is either 1 or 2.*

In the former case either $G \simeq D_8$ or $G \simeq \mathcal{C}_4 \times \mathcal{C}_2$; in the latter case G is an infinite nilpotent group of class 3 such that:

(i) $G' = \operatorname{tor} G$ is a noncyclic group of order 4;

(ii) G_{ab} is an abelian torsion-free group whose automorphism group is finite and has exponent 4 or 12;

(iii) $G = HL$, where H is isomorphic to the group G_0 described in Section 2 and L is a torsion-free abelian subgroup of $Z(G)$.

Proof — By a previous lemma $p^\lambda = 2$. The case in which $\mu = 1$, that is, $\operatorname{Aut} G \simeq D_8$ is well-known, and we shall disregard it. So, going back to notation used thus far in this section, in view of what we have already proved, we may assume that $A \simeq \mathcal{C}_2 \wr \mathcal{C}_{2^\mu}$ for some integer $\mu > 1$.

We shall first prove that G is infinite. Assume that G is finite. The characteristic subgroups of G form a chain, as follows from Lemma 3.9 (i) and from the fact that Z has order 2 (Lemma 3.9 (iii)) and so is contained in every nontrivial characteristic subgroup of G. As $G^2 \leq M$ and $M^2 \leq Z$ by Lemma 3.9 (ii), the socle U of G^2 has index 2 at most in G^2. Since U is characteristic in G and $G' < G^2$ it follows that $G' \leq U$, hence $\exp G' = 2$. Consequences of this fact are:

$$\forall x, y \in M \quad \forall g \in G \qquad \begin{aligned} &[x, x^g] = 1, \\ &[x, g, y] = [y, g, x], \\ &[x, g^2] = 1 \Rightarrow [x, g, g] = 1. \end{aligned} \tag{$*$}$$

For, as $M^2 \leq Z$ we have $1 = [x^2, g] = [x, g]^x [x, g]$, so $[x, g]^x = [x, g]^{-1} = [x, g]$, which is equivalent to the first identity. By applying it to x, y and xy we have $1 = [x, x^g] = [y, y^g] = [xy, (xy)^g]$. Now M has nilpotency class 2 (at most), so $[xy, (xy)^g] = [x, y^g][y, x^g]$. Again, since $\exp G' = 2$ this means that $[x, y^g] = [y, x^g]$. But $[x, y^g] = \big[x, y[y, g]\big] = [y, g, x][x, y]$ and similarly $[y, x^g] = [x, g, y][y, x]$, which proves the second identity. Finally, if $[x, g^2] = 1$ then we have $1 = [x, g][x, g]^g$, so $[x, g] = [x, g]^{-1} = [x, g]^g$. Thus all of $(*)$ is proved.

Next we describe the structure of M. Recall that $|Z(M)/Z| = 2$, thus $|Z(M)| = 4$. This makes it impossible that $G' < Z(M)$, hence $Z(M) \leq G'$ and $Z(M) \simeq V_4$, the noncyclic group of order 4. In particular M is not abelian and $M^2 = M' = Z$. Let $c \in Z(M) \smallsetminus Z$. Then $M = L \times \langle c \rangle$ for some maximal subgroup L of M, which is immediately seen to be extraspecial.

Let $g \in G \smallsetminus M$ and $C = C_M(g^2)$. By Lemma 3.9 (iv), $\exp G_{\mathrm{ab}} > 2$, hence $g^2 \notin G'$; a fortiori $g^2 \notin Z(M)$. Since $|M'| = 2$ we have $|M/C| = 2$. The mapping $f : x \in M \mapsto [x, g]Z \in G'/Z$ is an epimorphism whose kernel is $Z_2(G) = G^2$, because M/Z is abelian (and by the same lemma). If $C^f \leq Z(M)/Z$ then $|C/G^2| \leq 2$ and $|G/G^2| \leq 8$, so that Lemma 3.9 (iv) once again shows that $\mu = 2$.

Suppose that $\mu > 2$. Then we may choose $x \in C$ such that $a := [x, g] \notin Z(M)$. Also, $[C, g, x] \neq 1$. Indeed, if $[C, g, x] = 1$ then $[a, C] = [x, g, C] = 1$ by $(*)$; since $a \notin Z(M)$ and $C \lessdot M$ we have $C = C_M(a)$. But in a group whose derived subgroup has order 2, two elements may have the same centralizer only if they are congruent modulo the centre. Hence $a^{-1}g^2 \in Z(M)$, which is a contradiction because $a \in G' \geq Z(M)$ and $g^2 \notin G'$. Having established this, we may choose $y \in C$ such that $b := [y, g]$ does not commute with x. From $(*)$ we obtain that $[a, x] = [b, y] = [a, g] = [b, g] = 1$, moreover $[a, b] = 1$ because G' is abelian. If $[x, y] \neq 1$ we may replace y with yb, which does commute with x—note that $[yb, g] = b$. Finally, $[a, y] = [x, g, y] = [y, g, x] = [b, x] \neq 1$ Now we have that $H := \langle x, y, a, b \rangle$ is the central product of the two nonabelian groups $\langle x, b \rangle$ and $\langle y, a \rangle$, that both have order 8, because $M^2 = Z$ has order 2. We know that a and b have order 2, because $\exp G' = 2$, (so our two groups are in fact dihedral) and we can redefine also x and y to make them have order 2: if, say, x has order 4 then replace it with bx: all the required properties are preserved (in particular, $[bx, g^2] = 1$) and bx has order 2. Similarly we may assume that $y^2 = 1$. Now let $K := C_M(H)$. Then M is the central product HK with $H \cap K = Z(H) = Z$. Clearly both H and K are g-invariant and $g^2 \in K$. We can define an automorphism of G by letting it act trivially on $\langle g \rangle K$ and as follows on the generators of H:

$$y \mapsto x \mapsto xyc \qquad\qquad b \mapsto a \mapsto ab$$

(recall that $c \in Z(M) \smallsetminus Z$). To check that the automorphism is well-defined, note that the images of the four generators x, y, a, b still have order 2, the mutual commutators are preserved as is the action of g (because $[c, g]$ is the generator of Z, hence $[c, g] = [a, y]$ and so $[xyc, g] = a^y b[c, g] = ab$). This automorphism clearly has order 3, and this is a contradiction. Therefore $\mu = 2$. Lemma 3.9 shows now that $|G| = 32$ and the above argument restricts the structure of G strongly. Indeed, the maximal subgroup M is a direct product of a nonabelian group of order 8 by a group of order 2. Again let $g \in G \smallsetminus M$. Since $g^2 \notin Z(M)$ the group G can be described as follows: $G = \langle g, h\rangle$, where $H := \langle g^2, h\rangle$ is nonabelian of order 8 and its normal closure is $M = H \times \langle c\rangle$, where $c = [g, h]$. There are three possibilities for the isomorphism type of such a group: H may be chosen to be isomorphic to D_8 or Q_8, the quaternion group of order 8, and, in the former case, g may be chosen to have order 8 or 4 (and this order is the exponent of G). These choices indeed provide three pairwise nonisomorphic groups. Direct inspection reveals that two of them (those of exponent 8) have 2^7 automorphisms, while the third one has automorphism group of the same order (2^6) as, but not isomorphic to $\mathcal{C}_2 \wr \mathcal{C}_4$. This shows that G cannot be finite.

Thus G is infinite. By Lemma 1.3 of [2], TG^2 is a proper (characteristic) subgroup of finite index in G containing T. Hence $T \le M$ by Lemma 3.2. Then $T^2 \le T \cap M^2 \le T \cap Z = S \le G'$, by Lemma 3.9 (*ii*) and (*iii*). This implies that G^2_{ab} is torsion-free, hence $G' = T \cap G^2$. Then $T \cap ZG' = G'(T \cap Z) = G' = T \cap G^2$. On the other hand $ZG' < G^2$ by Lemma 3.9 (*iv*). This yields that $TZ = TZG' < TG^2$ and so $G^2 \nleq TZ$, hence $TZ < G^2$ by part (*i*) of the same lemma. Consider the natural conjugation A-epimorphism $\sim\colon G \twoheadrightarrow I$ again. The image of $G^2 = Z_2(G)$ is $Z(I) = [B, \alpha_0] = [A'\langle\beta\rangle, \alpha_0] = [A'\langle\beta\alpha_0\rangle, \alpha_0] = [I, \alpha_0]$. Thus $[G, \alpha_0]Z = G^2 > TZ$. But the Hallett-Hirsch Theorem shows that $[G, \alpha^4] \le T$, hence $[G, \alpha_0]Z > [G, \alpha^4]Z$ and so $\alpha_0 \notin \langle\alpha^4\rangle$. Therefore $\mu < 3$, that is to say, $\mu = 2$.

We still have to justify statements (*i*)–(*iii*). That $T = G'$ is clear now, since we just showed that $G' = T \cap G^2$ and thereafter that $T < G^2$. Since $|G'Z/Z| = 2 = |S| = |G' \cap Z|$ we have that $|G'| = 4$. Now, $C_G(G')$ is a characteristic subgroup of index 2 in G, hence $C_G(G') = M$. Suppose that G' is cyclic, say $G' = \langle c\rangle$, and let $g \in G \smallsetminus M$. Then $c^g = c^{-1}$. It easily follows that $gM \mapsto c$ defines a derivation from G/M to G', hence G has an automorphism centralizing M and mapping g to gc. But this automorphism has order 4 while we know that $C_A(M) = Z(A)$ has order 2. By this contradiction $G' \simeq V_4$, hence (*i*) is proved. Next, $\mathrm{Aut}\, G_{\mathrm{ab}} = \mathrm{Aut}(G/T)$ is finite and, by the Hallett-Hirsch Theorem, its order divides 12. To prove (*ii*) we therefore only have to check that G/T has an automorphism of order 4. If this is false then $A/C_A(G/T)$ has exponent 2 (at most), hence A^2 centralizes G/T. On the other hand A^2 certainly does centralize T, which has order 4, hence $A^2 \le C_A(G/T) \cap C_A(T)$. But this latter intersection is abelian, while A^2 is not. This proves (*ii*). Finally, Lemma 3.9 shows that we can write G as $\langle a, b\rangle Z_2(G)$ for suitable $a, b \in G \smallsetminus M$. Then $c := [a, b] \in G' \smallsetminus Z$ and $[c, a] = [c, b]$ is the generator of $G' \cap Z = S$, because $C_G(G') = M$. It follows that $H := \langle a, b\rangle$ is isomorphic to the group G_0 defined in Section 2. As $|H/Z(H)| = 16 = |G/Z|$ (see Lemma 3.9 again), then $G = HZ$, but $T \le H$ and so $G = HL$, if L is any complement to S in Z. □

References

[1] J.E. Adney and Ti Yen, Automorphisms of a p-group, *Illinois J. Math.* **9** (1965) 137–143.

[2] G. Cutolo, H. Smith and J. Wiegold, p-groups of maximal class as automorphism groups, *Illinois J. Math.*, to appear.

[3] R. Faudree, A note on the automorphism group of a p-group, *Proc. Amer. Math. Soc.* **19** (1968) 1379–1382.

[4] L. Fuchs, 'Infinite Abelian Groups', vol. 2, Academic Press, New York, 1970.

[5] H. Heineken and H. Liebeck, On p-groups with odd order automorphism groups, *Arch. Math. (Basel)* **24** (1973) 464–471.

[6] H. Heineken and H. Liebeck, The occurrence of finite groups in the automorphism group of nilpotent groups of class 2, *Arch. Math. (Basel)* **25** (1974) 8–16.

[7] B Huppert, 'Endliche Gruppen', Bd. I, Springer, Berlin, 1967.

[8] R. Lawton, A note on a theorem of Heineken and Liebeck, *Arch. Math. (Basel)* **31** (1978/79) 520–523.

[9] J.C. Lennox and S.E. Stonehewer, 'Subnormal subgroups of groups', Clarendon Press, Oxford, 1987.

[10] U.H.M. Webb, The occurrence of groups as automorphisms of nilpotent p-groups, *Arch. Math. (Basel)* **37** (1981) 481–498.

[11] G. Zurek, Eine Bemerkung zu einer Arbeit von Heineken und Liebeck, *Arch. Math. (Basel)* **38** (1982) 206–207.